IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	CASE NO.: 1:20CR441
	)	
Plaintiff,	)	JUDGE JAMES S. GWIN
	)	
v.	)	
	)	
BLESSING ADELEKE,	)	GOVERNMENT'S SENTENCING
	)	MEMORANDUM
Defendant.	)	

Now comes the United States of America, by and through its attorneys, Michelle M. Baeppler, First Assistant United States Attorney, and Brian S. Deckert and Daniel J. Riedl, Assistant United States Attorneys, and hereby files this sentencing memorandum. The Government agrees with the calculations contained within the Presentence Investigation Report filed December 22, 2022. (Doc. 71: PSR, PageID 527-549). The Government recommends a term of 60 months in accordance with the following memorandum.

I. OFFENSE CONDUCT AND GUIDELINE CALCULATION

A. Offense Conduct

The Defendant is a national of Nigeria and served as an administrator of the Shad0w.info carding forum and was a carder. Shad0w.info was an online marketplace where vendors of compromised data – such as credit card numbers, online accounts, or personally identifiable information (PII) – sold that compromised data to buyers to use for financial gain.

Some of the items listed for sale in Shad0w.info included user accounts at Amazon, eBay, Match.com, PayPal, email/password combinations from accounts from the United States and United Kingdom, credit cards including American Express, MasterCard, and Visa. Shad0w.info forum also listed for sale the credit card information for individual victims with

addresses in the Northern District of Ohio, Eastern Division, including addresses in Painesville, Mayfield Heights, and Lakewood, Ohio.

The Defendant, and others on the marketplace, obtained stolen credit card information, harvested credit card numbers, Bank Identification Numbers ("BINs"), security questions, and other data, including names of the account holders and PIN numbers for the credit cards. The Defendant, and others on the marketplace, then used the stolen card information to purchase items for themselves, including retail goods and gift cards. The Defendant shared this credit card information with others, on the Internet through ICQ, Facebook Messenger, email, and other social media applications. The Defendant then shipped retail goods and gift cards purchased with stolen card information to droppers. In some cases, the droppers converted the retail goods and gift cards to cash by returning them to retail stores for cash. In some cases, the droppers would forward the retail goods to another dropper provided by the Defendant. The Defendants eventually forwarded the retail goods, gift cards and currency, either by shipping or through electronic funds transfers, to members of the conspiracy for their personal enrichment.

On or about June 8, 2015, the Defendant caused sixteen (16) unauthorized checks totaling $19,180 to be issued from the Key Bank account of W.C.M., a resident of Pepper Pike, Ohio, to co-conspirators. The Defendant transmitted stolen credit card information to co-conspirator Harlow who utilized the stolen information to obtain merchandise and/or gift cards and sent money back to the Defendant. The Defendant utilized stolen banking information to transfer money to bank accounts of co-conspirators, who would send money back to the Defendant. Co-defendant Harlow received $10,000 in one deposit via this scheme. The Defendant sent four (4) Dell laptops purchased using stolen credit card information to co-defendant Harlow with the

expectation that the laptops would be sold and money would be sent back to him. The estimated value for each laptop was $600 for a total amount of $2,400.

Co-defendant Harlow transmitted $12,701 via Western Union and Moneygram to the Defendant as part of these schemes. The amount of loss attributable to the Defendant for the schemes involving co-Defendant Harlow alone totaled more than $40,000.

Testimony at trial revealed that the Defendant utilized threats of physical harm to a co-conspirator who expressed a desire to terminate her participation in the conspiracy.

B. Guideline Calculation

The PSR set forth the following computation of the Defendant's advisory sentencing guidelines:

Counts 1, 2 - 17: Conspiracy to Commit Bank Fraud, 18 U.S.C. § 1349 & Bank Fraud, 18 U.S.C. 1344		
Base offense level	7	§ 2B1.1(a)(1)
Loss (> $40,000)	+6	§ 2B1.1(b)(1)(D)
10 or more victims	+2	§ 2B1.1(b)(2)(A)(i)
Sophisticated means	+2	§ 2B1.1(b)(10)
Trafficking of unauthorized or counterfeit access device	+2	§ 2B1.1(b)(11)(B)(i)
Organizer, leader, manager, or supervisor	+2	§ 3B1.1(c)
Total Offense Level	**21**	

The Defendant did not have any criminal convictions and therefore his criminal history category is I. (Doc. 71: PSR, PageID 539). With an offense level 21 and a criminal history category of I, the Defendant's guideline imprisonment range is 37 to 46 months and is in zone D.

II. SENTENCING FACTORS 18 U.S.C. § 3553(A)

Upon properly calculating the advisory guideline range, this Court is required to follow 18 U.S.C. § 3553(a), which states:

> This Court is required to consider the following factors in determining the sentence.
>
> (a) Factors to be considered in imposing a sentence.--The court shall impose a sentence sufficient, but not greater than necessary,

> to comply with the purposes set forth in paragraph (2) of this subsection. The court, in determining the particular sentence to be imposed, shall consider--
>
> > (1) the nature and circumstances of the offense and the history and characteristics of the defendant;
> >
> > (2) the need for the sentence imposed--
> >
> > > (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
> > >
> > > (B) to afford adequate deterrence to criminal conduct;
> > >
> > > (C) to protect the public from further crimes of the defendant; and
> > >
> > > (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner;
> >
> > (3) the kinds of sentences available;
> >
> > (4) the kinds of sentence and the sentencing range established for--
> >
> > (5) any pertinent policy statement--
> >
> > (6) the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and
> >
> > (7) the need to provide restitution to any victims of the offense.

18 U.S.C. § 3553(a).

The PSR identified two grounds for an upward variance from the applicable guidelines in this matter. First, the total loss applied in the guidelines involved only a small portion of the total scheme operated by the Defendant. (Doc. 71: PSR, PageID 547). Second, the Defendant threatened a co-conspirator who expressed a desire to exit the conspiracy. (*Id.*). The government agrees with those grounds.

A. The Full Extent of Defendant's Relevant Conduct Warrants an Upward Variance.

The Defendant operated multiple different fraud schemes involving the two co-conspirators who testified at trial. At the most basic level, the Defendant utilized stolen bank account and credit card information to obtain monies. That information was utilized to purchase gift cards and merchandise that were sold or converted into currency and sent back to the Defendant. The Defendant also sent money directly to the bank account of a co-conspirator and the money was withdrawn before the fraudulent transfer was detected. In this case, the Defendant sent $10,000 to co-defendant Harlow, however, the intended loss for this scheme was much higher. The Defendant informed the co-conspirators that he intended to send a total of $84,000 from the account. (See Exhibit 2)

The Facebook records demonstrate that the Defendant was operating this identical scheme with other droppers. For example, one Facebook user sent wire transfers of $550, $600, and $900 to the Defendant. (See Exhibit 1). The Defendant had fraudulent access to multiple bank accounts, knew the balances of the accounts, sent the information to the droppers, and it was his intention to withdraw as much as possible before access was cut off. (See Exhibit 2). A review of the Facebook records and Gmail account revealed that the Defendant had fraudulent access to over $800,000 in funds. (See Exhibit 2). Given the context in which the available funds were discovered and the Defendant's proven history of theft, it is reasonable to conclude that the Defendant did or intended to steal all of the funds in those accounts. The Defendant argues that intended loss should not be applied in this case as it is contained in the application note for U.S.S.G. § 2B1.1. (Doc. 74: Deft. Sent. Mem., PageID 565-67). The Sixth Circuit has consistently concluded that intended loss is a valid method to calculate loss under U.S.S.G.

§ 2B1.1. Indeed, the Sixth Circuit held that intended loss can include the full amount of a deposited fraudulent check even though the perpetrator was only able to withdraw less than one percent of the full amount. *See United States v. Thomas*, 841 Fed. Appx. 934, 938 (6th Cir. 2021) ("It is reasonable to infer that Thomas intended to continue, and would have continued, withdrawing and utilizing additional funds from the check had the bank not intervened and frozen the account.") In this case, the evidence demonstrates that the Defendant intended to obtain as much of the funds located in the bank accounts as possible and therefore, the full amounts of those accounts can be considered by this Court for an upward variance.

The Defendant also states in his sentencing memorandum that the Defendant should not receive a 2-level enhancement for mass marketing pursuant to U.S.S.G. § 2B1.1(b)(2)(A), but concedes that the enhancement should apply because there were more than ten victims. (Doc. 74: Deft. Sent. Mem., PageID 567). The government agrees. The Defendant's Facebook account contains well over 10 victims' information that he sent to others for the purposes of fraud. There are over 30,000 pages of records of the DetectedBits Facebook account and it is virtually all fraud related. Additionally, the Defendant was an administrator of an online marketplace in which investigators discovered credit card information for sale from 1,277 unique victims. Given these facts, there were far more than 10 victims and the 2-level enhancement is properly applied.

The actual loss amount attributable to the Defendant in the PSR is limited to the fraudulent activity involving co-defendant Harlow. A review of the Facebook records shows that the Defendant's involvement in fraud was much more pervasive than the guideline sentence captures, and an upward variance is appropriate.

B. The Defendant Utilized Threats and Intimidation to Maintain Control Over His Droppers.

A witness testified at trial that when she expressed a desire to stop committing fraudulent activity on behalf of the Defendant, he became angry and threatening. The Facebook records confirm this pattern of behavior. (See Exhibit 3). On September 3, 2015, the Defendant transmitted to co-defendant Harlow $10,000 into her bank account and with the apparent expectation that she would withdraw the money and send it back to him via Western Union or Moneygram. Co-defendant Harlow did not send the money back to the Defendant as expeditiously as he expected, which led to threats and intimidation. On September 10, 2015, the Defendant sent a Facebook communication to Harlow in which he stated that the money was for someone else and that this person had a friend that lived in New York and will "check out [Harlow's] address." On September 11, 2015, the Defendant employed another dropper located in the United States to call co-defendant Harlow and "put fire on her a—right now." (See Exhibit 5). The dropper sent a screenshot to the Defendant containing a text communication the dropper had with Harlow. In that screenshot, the dropper tells Harlow that she has Harlow's address, she lives in New York, and is only 7 ½ hours away. Later that day,, the Defendant sent Harlow a Facebook communication that stated "I will put in every resources to make u pay dearly for this." Additionally, the Defendant stated, "If I get back at you and put u in a mess," and "Ur kids will suffer."

The Defendant's pattern of threats and intimidation recurred throughout his dealings with associates and droppers under his control. For example, on December 5, 2014, the Defendant was upset at one of the droppers employed by an associate of his and stated, "I swear if your friend dont send the money. I will f--- him up big time." Further, the Defendant stated, "I will not ask again. next thing he will see is action. and I will also blame you too for it because its your

friend you brought him to me." The dropper eventually sent $550 by Moneygram to the Defendant.

There is not a specific offense characteristic that addresses the use of threats and intimidation in the Guidelines. The nature and circumstances of the offense as set forth in 18 U.S.C. § 3553(a) does provide for the Court to consider this kind of behavior when fashioning an appropriate sentence. For this reason, the government believes that the nature and circumstances of the offense supports an upward variance of the guidelines sentence.

III. CONCLUSION

Based upon the serious nature of the offense conduct, the uncaptured scope of the Defendant's criminal schemes, and his use of threats and intimidation during the conspiracy, the Government respectfully requests this Court sentence the Defendant above the advisory guideline range to a term of 60 months.

Respectfully submitted,

MICHELLE M. BAEPPLER
First Assistant United States Attorney

By: /s/ Brian S. Deckert

Brian S. Deckert (OH: 0071220)
Assistant United States Attorney
United States Court House
801 West Superior Avenue, Suite 400
Cleveland, OH 44113
(216) 622-3873
(216) 522-8355 (facsimile)
Brian.Deckert@usdoj.gov